# 5 FAM 460
# THE PRIVACY ACT AND PERSONALLY IDENTIFIABLE INFORMATION

*(CT:IM-156; 10-01-2014)*
*(Office of Origin: A/GIS/IPS)*

## 5 FAM 461 SCOPE

*(CT:IM-156; 10-01-2014)*

This section addresses the requirements of the Privacy Act of 1974, as amended; E-Government Act of 2002, Section 208; Office of Management and Budget (OMB) directives *and guidance* governing privacy; and Department policies concerning the collection, use, maintenance, and dissemination of personally identifiable information (PII).

## 5 FAM 462 AUTHORITIES

### 5 FAM 462.1 Statutory

*(CT:IM-156; 10-01-2014)*

Statutory authorities pertaining to privacy include:

*(1)* Privacy Act of 1974, as amended (5 U.S.C. 552a);

*(2)* E-Government Act of 2002, Section 208 *(*44 U.S.C. 3501 *note);*

*(3)* *Federal Information Security Management Act of 2002 (FISMA) (*44 U.S.C. 3541 *et. seq.);*

*(4)* *Information Technology Management Reform Act of 1996 (ITMRA) (Clinger-Cohen Act), as amended (Public Law 104-106, 110 Stat. 679 (1996));*

*(5)* Freedom of Information Act of 1966 *(FOIA),* as amended; privacy exemptions (5 U.S.C. 552(c)(6) and (*c*)(7)(*C*));

*(6)* Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501 et seq.);

*(7)* Children's' Online Privacy Protection Act (COPPA) of 1998 (Public Law 105-277).

*(8)* *Fair Credit Reporting Act of 1970, Section 603 (*15 U.S.C. 1681a)*; and*

*(9)* Executive Order 13526 *or predecessor and successor Executive Orders on*

*classifying national security information regarding covert operations and/or confidential human sources.*

## 5 FAM 462.2 Office of Management and Budget (OMB) Guidance

*(CT:IM-156; 10-01-2014)*

OMB *directives and* guidance *include*:

(1) OMB Privacy Act Implementation: Guidelines and Responsibilities, published in the Federal Register, Vol. 40, No. 132, Part III (July 9, 1975);

(2) Privacy and Personal Information in Federal Records, M-99-05, *Attachment A* (May 14, 1998);

(3) *Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records," M-99-05 (January 7, 1999);*

(4) Privacy Policies on Federal websites*,* M*-99-18 (June 2, 1999);*

*(5)* Management of Federal Information Resources, Circular No. A-130, Transmittal Memorandum No. 4 *(Nov.* 28, 2000*);*

(6) OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22 (Sept. 26, 2003);

(7) Designation of Senior Agency Officials for Privacy, M-05-08 (Feb. 11, 2005);

(8) Safeguarding Personally Identifiable Information, M-06-15 (May 22, 2006);

(9) Protection of Sensitive Agency Information, M-06-16 (June 23, 2006);

(10) Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, M-06-19 (July 12, 2006);

*(11) Recommendations for Identity Theft Related Data Breach Notification (Sept. 20, 2006);*

*(12)* Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16 (May 22, 2007);

*(13) Social Media, web-Based Interactive Technologies, and the Paperwork Reduction Act (April 7, 2010);*

*(14) Guidelines for Online Use of Web Measurement and Customization Technologies, M-10-22 (June 25, 2010);*

*(15) Guidance for Agency Use of Third-Party Websites and Applications, M-10-23 (June 25, 2010); and*

*(16) Sharing Data While Protecting Privacy, M-11-02 (Nov. 3, 2010).*

# 5 FAM 463 DEFINITIONS

*(CT:IM-156; 10-01-2014)*

**Availability:** Timely and reliable access to and use of information (see the E-Government Act of 2002, Section 3542).

**Best judgment standard:** *An assessment* in context of the sensitivity of personally identifiable information (PII) and any actual or suspected breach of such information for the purpose of deciding whether reporting a breach is warranted.

***Biennial System of Records Notice (SORN) Review:*** *A review of SORNs conducted by an agency every 2 years following publication in the Federal Register, to ensure that the SORNs continue to accurately describe the systems of records.*

**Breach:** The loss of control, compromise, unauthorized disclosure, *unauthorized* acquisition, *unauthorized* access, or any similar term referring to situations in which persons other than authorized users *or authorized persons* for an other than authorized purpose, have access or potential access to PII, whether physical or electronic.

**Breach analysis:** The process used to determine *whether* a data breach may result in the misuse of PII or harm to the individual.

**Breach notification:** The process of notifying *only those* individuals who may be adversely affected by a breach of their PII.

***Breach response policy (BRP):*** *The process used to determine if a data breach may result in the potential misuse of PII or harm to the individual.*

***Breach response procedures:*** *The operational procedures to follow when responding to suspected or confirmed compromise of PII, including but not limited to: risk assessment, mitigation, notification, and remediation.*

**Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (see the E-Government Act of 2002, Section 3542).

**Core response group (CRG):** A Department group established in accordance with the recommendations of the Office of Management and Budget (OMB) and the President's Identity Theft Task Force concerning data breach notification.

**Computer emergency readiness team (US-CERT):** The operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS) charged with providing response support and defense against cyber attacks.

***Cyber* incident response team (DS-CIRT):** The central point in the *Department* of *State* for reporting computer security incidents (including *privacy incidents in all formats such as* hard copy) that occur on the

Department of State networks, including incidents involving PII.

***Disclosure:*** *Providing information from a system of records, by any means, to anyone other than the individual by whose name or other identifier the record is retrieved.*

**E-Government Act of 2002, Section 208:** A statutory provision that requires sufficient protections for the privacy of personally identifiable information (PII) by requiring agencies to assess the privacy impact of all substantially revised or new information technology (IT) systems as agencies implement citizen-centered electronic government.

**Federal Information Security Management Act (FISMA):** Title III of the E-Government Act of 2002 that requires Federal agencies to adhere to certain information security standards for all information systems under their control.

**Freedom of Information Act (FOIA):** A *Federal* law that provides that any person has the right, enforceable in Federal Court, to obtain access to Federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.

**Harm:** *Damage, loss*, or *misuse of information which adversely affects* one or more individuals or undermines the integrity of a system or program.

**Identity theft:** "A fraud committed using the identifying information of another person," as specified under Section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

**Individual:** A citizen of the United States or an alien lawfully admitted for permanent residence.

**Integrity:** Safeguards against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

**National Security System (NSS)** *(as defined by the Clinger-Cohen Act):* A *telecommunication or information system operated by the Federal Government,* the function, operation or use of which involves: intelligence activities; cryptologic activities related to national security; command and control of military forces; *involves* equipment that is an integral part of a weapon or weapons systems; or *systems critical to* the direct fulfillment of military or intelligence missions, *but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management.*

**Need to know***: Any workforce members of the Department who maintain the record and who have a need for the record in the performance of their official duties.*

**Nonrepudiation:** *The Department's protection* against an individual falsely denying having performed a particular action. This provides the capability to determine whether a given individual took a particular action such as creating

information, sending a message, approving information, and receiving a message.

***Non-U.S. Person**: A person who is neither a citizen of the United States nor an alien lawfully admitted for permanent residence.*

***Notification**: Notice sent by the notification official to individuals or third parties affected by a breach. This may be accomplished via telephone, email, written correspondence, or other means, as appropriate.*

***Notification Official**: The Department official who authorizes or signs the correspondence notifying affected individuals of a breach.*

**Personally identifiable information (PII) *(as defined by OMB M-07-16):*** Information *that* can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

**Privacy Act of 1974, as amended:** A *Federal* law that establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of *personal* information about individuals that is maintained in systems of records by Federal agencies*, herein identified as the Privacy Act*.

**Privacy impact assessment (PIA):** An analysis of how information is handled:

(1) To ensure *compliance with* applicable legal, regulatory, and policy requirements regarding privacy;

(2) To determine the risks and effects of collecting, maintaining and disseminating information in identifiable form; and

(3) To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Privacy protection governance board (PPGB):** An Assistant Secretary-level Department group established to ensure the Department is positioned to respond to relevant directives and other authorities concerning the protection of personally identifiable information (PII) in a unified manner, fully integrating the requirements of all Department business operations.

**Record (as defined by the Privacy Act):** Any item, collection, or grouping of information about an individual that is maintained by a Federal agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

**Routine use:** The condition of disclosure *under* the Privacy Act that permits a Federal agency to disclose Privacy Act protected information when to do so is compatible with the purpose for which it was collected.

**Rules of behavior:** Established rules developed to promote a workforce member's understanding of the importance of safeguarding personally identifiable information (PII), his or her individual role and responsibilities in protecting PII, and the consequences for failed compliance. All workforce members with access to PII in the performance of their official duties are required to comply with established rules.

**Sensitive personally identifiable information:** Personal information that specifically identifies an individual and, if such information is exposed to unauthorized access, may cause harm to that individual at a moderate or high impact level (see 5 FAM 1065.4 for the impact levels.)

**Supervisor:** A manager (e.g., oversight manager, task manager, project leader, team leader, etc.), contract officer representative (COR), or any other person who has the authority to assign official duties and/or work assignments to the workforce members. Supervisors are also workforce members.

**System of Records:** A group of any records (as defined by the Privacy Act) under the control of any Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

**System of Records Notice (SORN):** A *formal* notice to *the public* published in the Federal Register *that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by the Department.*

***Unauthorized access:*** *Logical or physical access without a need to know to a Department network, system, application, data, or other resource in any format.*

**Unauthorized disclosure:** Disclosure*, without authorization, of information in the possession of the Department that is about or referring to an individual.*

**Workforce member:** Department employees, contractors (commercial and personal service contractors), U.S. Government personnel detailed or assigned to the Department, and any other personnel *(i.e. locally employed staff)* who perform work for or on behalf of the Department.

# 5 FAM 464 PRIVACY ACT

*(CT:IM-156; 10-01-2014)*

a. All workforce members must safeguard *personally identifiable* information *(PII)* when collecting, maintaining, using and disseminating information and make such information available to the individual upon request in accordance with the provisions of the Privacy Act.

b. The Privacy Act requires each Federal agency that maintains a system of

records to:

(1) The greatest extent practicable, collect information about an individual directly from the individual if the information may be used to make decisions with respect to the individual's rights, benefits, and privileges under Federal programs;

(2) Collect and maintain information on individuals only when it is relevant and necessary to the accomplishment of the Department's purpose, as required by statute or Executive Order;

(3) Maintain information in a system of records that is accurate, relevant, timely, and complete as possible to ensure fairness to the individual;

(4) *Submit a System of Records Notice (SORN) to the Federal Register for publication* at least 40 days prior to creation of a new system of records or significant alteration to an existing system*;*

*(5) Conduct a biennial review (every 2 years) following a SORN's publication in the Federal Register to ensure that Department SORNs continue to accurately describe the systems of records;*

*(6)* Make certain all Department forms used to collect information from individuals subject to the Privacy Act contain a Privacy Act Statement that includes:

(a) The statute or Executive Order authorizing the collection of the information;

(b) The purpose for which the information will be used, as authorized through statute or other authority;

(c) Potential disclosures of the information outside the Department of State;

(d) Whether the disclosure is mandatory or voluntary; and

(e) Consequences, if any, to the individual for not providing the requested information;

(*7*) Ensure an individual is not denied any right, benefit, or privilege provided by law for refusing to disclose their Social Security number, unless disclosure is required by Federal statute;

(*8*) Make certain *an* individual's personal information is properly safeguarded and protected from unauthorized disclosure (e.g., use of locked file cabinet, password-protected systems); and

(*9*) Ensure that information is not disclosed from records maintained in a system of records to any person or agency ***except*** with the written consent of the individual to whom the record pertains. Written consent is ***not*** required under certain circumstances when disclosure is:

(a) To workforce members of the agency on a "need to know" basis;

(b) Required under the Freedom of Information Act (FOIA);

(c) For a routine use as published in the Federal Register (contact A/GIS/IPS/PRV for specific information concerning "routine uses");

(d) To the U.S. Bureau of Census;

(e) For statistical research;

(f) To the National Archives and Records Administration (NARA);

(g) For law enforcement purposes, but only pursuant to a request from the head of the law enforcement agency or designee;

(h) For compelling cases of health and safety;

(i) To either House of Congress or authorized committees or subcommittees of the Congress when the subject is within its jurisdiction;

(j) To the Government Accountability Office (GAO);

(k) Required under court order; or

(l) Pursuant to the Debt Collection Act; and

*(m) As disclosed in the current SORN as published in the Federal Register.*

c. In addition, all managers of record system(s) must keep an accounting for 5 years after any disclosure or the life of the record (whichever is longer) documenting each disclosure, *except disclosures made as a result of* a "need-to-know" within the agency or FOIA disclosure. Each accounting must include the date, nature, and purpose of disclosure, and the name and address of the person or agency to whom the disclosure was made.

# 5 FAM 465 CIVIL AND CRIMINAL PENALTIES

*(CT:IM-156; 10-01-2014)*

The Privacy Act of 1974, as amended, imposes penalties directly on individuals if they knowingly and willingly violate certain provisions of the Act. All managers of record systems are responsible for *ensuring that* workforce members *who work* with *Department record systems are* fully aware of these provisions and the corresponding penalties.

# 5 FAM 466 PRIVACY IMPACT ASSESSMENT (PIA)

*(CT:IM-156; 10-01-2014)*

a. The E-Government Act of 2002, Section 208, requires a Privacy Impact assessment (PIA) on information technology (IT) systems collecting or maintaining electronic information *on* members of the public. The public, in

accordance with the *purpose of the* E-Government Act, includes U.S. citizens and aliens lawfully admitted for permanent residence*. Although Section 208 specifically excludes* Department *employees,* the *Department has expanded the PIA* requirement to *cover* systems that collect or maintain electronic information about *all* Department *workforce members.*

b. A PIA is an analysis of how information is handled to:

(1) Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) Determine the risks and effects of collecting, maintaining, and disseminating personally identifiable information (PII) in a system; and

(3) Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

*c.* The PIA is also a way the Department maintains an inventory of its PII holdings, which is an essential responsibility of the Department's privacy program. For systems that collect information from or about the public, the Privacy Division (A/GIS/IPS/PRV) posts these collections on the Department's Internet website as notice to the public of the existence and character of the system*.*

d. A PIA must be conducted in any of the following circumstances:

(1) For a new system;

(2) *The* modification *of* an existing system that may create privacy risks;

(3) *When an* update *to* an existing PIA as required for a system's triennial security reauthorization; and

*(4) Whenever an agency's use of a third-party website or application makes PII available to the agency.*

e. A PIA is not required for National Security Systems (NSS) as defined by *the Clinger-Cohen Act of 1996.*

# 5 FAM 467 BREACH RESPONSE POLICY (BRP)

## 5 FAM 467.1 Purpose

*(CT:IM-156; 10-01-2014)*

*a. The policy contained herein is in response to the Federal mandate prescribed in the Office of Management and Budget's Memorandum (OMB) 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," which requires agencies to report all incidents involving personally identifiable information (PII) to US-CERT within one hour of discovering the incident.*

*Additionally, this policy complies with the requirements of OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," that all agencies develop and implement a breach notification policy.*

b. *As outlined in* 5 FAM 463*, the term Breach Response Policy includes all aspects of a privacy incident/breach relating to the reporting, responding to, and external notification of individuals affected by a privacy breach/incident.*

c. *The breach reporting procedures located on the privacy division website describe the procedures an individual must follow when responding to a suspected or confirmed compromise of PII.*

## 5 FAM 467.2 Policy

*(CT:IM-156; 10-01-2014)*

a. *The Department's Breach Response Policy is that all incidents involving personally identifiable information (PII) shall be reported to US-CERT within one hour of discovering the incident. This requirement is in compliance with the guidance set forth in Office of Management Budget Memorandum M-06-19.*

b. *If an incident contains classified material it also is considered a "security incident." Reporting requirements and detailed guidance for security incidents are in* 12 FAM 550*, Security Incident Program.*

c. *Except in cases where classified information is involved, the office responsible for a breach, as determined by the Director, Office of Information Programs and Services (A/GIS/IPS), is required to conduct an administrative fact-finding task to obtain all pertinent information relating to the breach. The Bureau of Diplomatic Security (DS) will investigate all breaches of classified information. Additionally, the responsible office is required to complete all appropriate response elements (risk assessment, mitigation, notification and remediation) to resolve the case. The IPS Director has the final authority to determine that all breach response action items have been completed and that the case can be closed.*

d. *The Department's Privacy Division (A/GIS/IPS/PRV) is responsible to provide oversight and guidance to offices in the event of a breach.*

## 5 FAM 467.3 Privacy Protection Governance Board

*(CT:IM-156; 10-01-2014)*

a. The Privacy Protection Governance Board (PPGB) *was established to address issues relating to personally identifiable information (PII) from a Department-wide perspective and to ensure the Department's ability to respond uniformly to law, regulations and policies concerning the safeguarding of PII.*

b. *The PPGB addresses interdependencies among security, privacy, and*

*technology when examining the collection, use, maintenance, and dissemination of PII.*

## 5 FAM 467.3-1 Purpose

*(CT:IM-156; 10-01-2014)*

*The Privacy Protection Governance Board (PPGB):*

*(1) Provides broad program oversight, as appropriate, and serves as the Department's focal point for protecting personally identifiable information (PII) and privacy interests;*

*(2) Supports and oversees the work of the Core Response Group (CRG);*

*(3) Develops guidance relating to implementation and execution of privacy-related programs requiring senior-level decisions that impact Department-wide operations and activities, such as breach notification;*

*(4) Appoints representatives and subject matter experts nominated by member bureaus for working groups to identify issues that may need PPGB consideration; and*

*(5) Increases workforce members' awareness of the Department's privacy policies to ensure that adequate controls are in place (e.g., proper handling of PII on laptops and other mobile storage devices, appropriate marking of privacy-protected information to maintain adequate controls, etc.).*

## 5 FAM 467.3-2 Organization

*(CT:IM-156; 10-01-2014)*

*a. The Privacy Protection Governance Board (PPGB) membership is intentionally broad enough to ensure that all facets of personally identifiable information (PII) within the Department (e.g., privacy, personnel management, operations, security, information technology, and legal concerns) are addressed, and that the Department's subject matter experts in these areas can establish viable and integrated privacy policies.*

*b. Each member shall designate a primary representative and primary substitute member with suitable subject matter expertise to serve on the Core Response Group (CRG), on behalf of the PPGB. The appointed representatives will be responsible for providing recommendations and/or proposals for addressing specific privacy issues to include PII within their respective business area.*

*c. PPGB membership. At a minimum, membership shall include:*

*(1) Assistant Secretary for Administration (A), (PPGB Chair);*

*(2) The Office of the Under Secretary for Management (M) and the Office of Management Policy, Rightsizing and Innovation (M/PRI);*

*(3) Assistant Secretary for the Bureau of Diplomatic Security (DS);*

*(4) Chief Information Officer/Bureau of Information Resource Management (IRM/CIO);*

*(5) Comptroller, Bureau of the Comptroller and Global Financial Services (CGFS);*

*(6) Assistant Secretary for Public Affairs (PA);*

*(7) Assistant Secretary for the Bureau of Consular Affairs (CA);*

*(8) Director General of the Foreign Service and Director of Human Resources (M/DGHR);*

*(9) Medical Director (MED);*

*(10) Deputy Legal Adviser (L); and*

*(11) Assistant Secretary for the Bureau of Legislative Affairs (H).*

*d. PPGB Executive Secretary. The Director, Office of Information Programs and Services (A/GIS/IPS) will be a non-voting member of the PPGB.*

*e. Additional members. The Chairperson may augment the membership with representatives from other bureaus as needed.*

## 5 FAM 467.3-3 Coordination, Liaison, and Support Staff

*(CT:IM-156; 10-01-2014)*

*Individual bureaus may provide program, technical, legal, and administrative support, as needed, by the Privacy Protection Governance Board (PPGB).*

## 5 FAM 467.3-4 Meetings

*(CT:IM-156; 10-01-2014)*

*The Privacy Protection Governance Board (PPGB) holds formal meetings as needed to discuss privacy issues or potential privacy concerns in Department programs or major initiatives. The PPGB ensures that all recommendations sustain and enhance the Department's privacy objectives. Further, it directs the establishment of additional technical support teams, working groups, and/or committees, as it deems necessary, to address specific privacy issues. The Executive Secretary must coordinate meeting agendas, prepare and maintain meeting minutes, and provide administrative support as deemed necessary.*

# 5 FAM 467.4 Core Response Group (CRG)

*(CT:IM-111; 07-12-2010)*

The PPGB established the Core Response Group (CRG) in accordance with the Office of Management and Budget (OMB) Memorandum M-07-16 and recommendations from the President's Identity Theft Task Force.

## 5 FAM 467.4-1 Purpose

*(CT:IM-156; 10-01-2014)*

The Core Response Group (CRG) provides a mechanism for the Department to respond promptly and appropriately in the event of a data breach involving *personally identifiable information (PII) in accordance with the guidelines contained in OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, dated July 12, 2006; OMB Memorandum from the Identity Theft Task Force, dated September 19, 2006; and OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

## 5 FAM 467.4-2 Activities

*(CT:IM-156; 10-01-2014)*

a. In the event of a suspected or confirmed data breach involving, or potentially involving, personally identifiable information (PII), the *Director of the Office of Information Programs and Services (A/GIS/IPS), at their discretion, will convene the* Core Response Group (CRG). If the CRG determines that sufficient privacy risk to affected individuals exists, it will assist the relevant bureau or office responsible for the data *breach* with the appropriate response.

b. The CRG *uses* the criteria in 5 FAM 468 to direct or perform the following actions:

   (1) Perform a data breach analysis to determine the potential for harm;

   (2) If *potential for* harm *exists*, such as *if there is* a potential for identity theft, establish, in conjunction with the relevant bureau or office, a tailored response plan to address the risk, which may include notification to those potentially affected; *identifying* services the Department may provide to those affected; and/or a public announcement;

   (3) Assist the relevant bureau or office in executing the response plan, including providing technical, administrative, and operational support on the privacy and identity theft aspects of the breach;

   (4) Ensure the Department maintains liaison as appropriate with outside agencies and entities (e.g., U.S. Computer Emergency Readiness Team (US-CERT), the Federal Trade Commission (FTC), credit reporting bureaus, members of Congress, and law enforcement agencies);

   (5) Develop a notification strategy including identification of a notification official, and establish liaisons to work with Department bureaus, other Federal agencies, and private-sector entities to quickly address notification issues within its purview;

   (6) Keep the Privacy Protection Governance Board (PPGB) informed of

response to any data breach and report to, and seek guidance from, the PPGB, as necessary; and

(7) Provide comprehensive reports to the PPGB, as necessary, regarding actions taken in response to potential or actual data breaches involving *PII.*

## 5 FAM 467.4-3 Membership

*(CT:IM-156; 10-01-2014)*

The *Director of the Office of Information Programs and Services (A/GIS/IPS) is designated* the Chair of the Core Response Group (CRG). In addition, the CRG will consist of representatives from the following bureaus:

(1) Bureau of Diplomatic Security (DS);

(2) Bureau of Information Resource Management (IRM);

(3) Bureau of the Comptroller and Global Financial Services (CGFS);

(4) Bureau of Consular Affairs (CA);

(5) Bureau of Public Affairs (R);

(6) Medical Director (MED);

(7) Office of the Legal Adviser (L);

(8) Director General of the Foreign Service and Director of Human Resources (M/DGHR); and

(9) Bureau of Legislative Affairs (H).

## 5 FAM 467.4-4 Roles

*(CT:IM-156; 10-01-2014)*

a. Bureau representatives and subject-matter experts will participate in the data breach *analysis* conducted by the Core Response Group (CRG) in order to determine the scope and gravity of the data breach and the impact on individual(s) based on the type and context of information compromised.

b. The notification official will work with appropriate bureaus to review and reassess, if necessary, the sensitivity of the compromised information to determine whether, when, and how notification should be provided to affected individuals.

c. CRG liaison coordinates with bureaus and external agencies for counsel and assistance throughout the process of bringing the breach to resolution.

## 5 FAM 467.4-5 Meetings

*(CT:IM-156; 10-01-2014)*

Meetings of the Core Response Group (CRG) *are* convened at the discretion of the Chair.

# 5 FAM 468 BREACH IDENTIFICATION, ANALYSIS, AND NOTIFICATION

## 5 FAM 468.1 Purpose

*(CT:IM-156; 10-01-2014)*

The purpose of breach identification, analysis, and notification is to establish criteria used to:

(1) Identify a breach of personally identifiable information (PII) in paper or electronic form;

(2) Assess the severity of a breach of PII in terms of the potential harm to affected individuals;

(3) Determine whether the notification of affected individuals is required or advisable; *and*

*(4) Identify whether the breach also involves classified information, particularly covert or intelligence human source revelations. If so, the Department's Privacy Coordinator will notify one or more of these offices: the* E.O. 13526 *Program Manager in A/GIS/IPS, the Office of the Legal Adviser (L/M), or the Bureau of Diplomatic Security (DS) for further follow-up.*

## 5 FAM 468.2 Roles

*(CT:IM-156; 10-01-2014)*

a. **Bureau of Administration:** The Assistant Secretary for Administration, as the Department's designated Senior Agency Official for Privacy (SAOP), has overall responsibility and accountability for ensuring that the Department's response to personally identifiable information (PII) breaches complies with *Federal legislation*, Executive Branch regulations and *internal Department policy*.

b. **Bureau of Diplomatic Security:**

(1) The *Cyber* Incident Response Team (DS-CIRT) is the Department's focal point for reporting suspected *or confirmed* breaches of sensitive PII (regardless of the medium of the information). Contact DS-CIRT at cirt@state.gov.; and

*(2) The Office of Information Security and/or the Office of Counterintelligence*

*and Investigations will conduct all investigations concerning the compromise of classified information.*

c. **Core Response Group (CRG):** The CRG will direct or perform breach analysis and breach notification actions.

## 5 FAM 468.3 Identifying Data Breaches Involving Personally Identifiable Information (PII)

*(CT:IM-156; 10-01-2014)*

a. *Department workforce members must report data breaches that include,* but are not limited to, those involving the following types *of personally identifiable information,* whether pertaining to *other* workforce members or members of the public:

(1) Personnel or payroll information;

(2) Social Security numbers and/or passport numbers;

(3) Date of birth, place of birth and/or mother's maiden name;

(4) Medical information;

(5) Law enforcement information that may identify individuals, including information related to investigations, arrests, convictions, or sentencing;

(6) Department credit card holder information or other information on financial transactions (e.g., garnishments);

(7) Passport applications and/or passports; or

(8) Biometric records.

b. Upon receipt of a notice of *a data breach incident involving* PII*, DS-CIRT will:*

(1) Notify US-CERT within one hour;

(2) Notify the Department's Privacy Division (A/GIS/IPS/PRV); and

(3) If a criminal act is suspected or confirmed, notify the Office of Inspector General, Office of Investigations (OIG/INV) either concurrent with or subsequent to notification to US-CERT.

## 5 FAM 468.4 Considerations When Performing Data Breach Analysis

*(CT:IM-111; 07-12-2010)*

Considerations when performing a data breach analysis include:

(1) The nature, content, and age of the breached data, e.g., the data elements involved, such as name, Social Security number, date of birth;

(2) The ability and likelihood of an unauthorized party to use the lost, stolen or

improperly accessed or disclosed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of any person;

(3) Ease of logical data access to the breached data in light of the degree of protection for the data, e.g., encrypted and level of encryption, or plain text;

(4) Ease of physical access to the breached data, e.g., the degree to which the data is readily available to unauthorized access;

(5) Evidence indicating that the breached data may have been deliberately targeted by unauthorized persons; and

(6) Evidence that the same or similar data had been acquired in the past from other sources and used for identity theft or other improper purposes.

## 5 FAM 468.5 Options After Performing Data Breach Analysis

*(CT:IM-156; 10-01-2014)*

a. Upon conclusion of a data breach analysis, the following options are *available to* the Core Response Group (CRG) for their applicability to the incident. The CRG will consider whether to:

(1) Notify affected individuals;

(2) Offer credit protection services to affected individuals;

(3) Notify an issuing bank if the breach involves U.S. Government authorized credit cards;

(4) Review and identify systemic vulnerabilities or weaknesses and preventive measures;

(5) *Identify any required remediation actions to be employed;*

(6) Take other measures to mitigate the potential harm; or

(7) *Take no further action and recommend the case be closed.*

b. The CRG *works* with appropriate bureaus *and offices* to review and reassess, if necessary, the sensitivity of the breached data to determine when and how notification should be provided or other steps that should be taken. The CRG must make any recommendation for notification to the Chair of the Privacy Protection Governance Board (PPGB), who may refer the matter to the full PPGB *and/*or, if necessary, the Under Secretary for Management (M).

c. If the CRG determines that there is minimal risk for the potential misuse of personally identifiable information (PII) involved in a breach, it *shall* advise the PPGB and take no further action unless the PPGB decides otherwise.

d. The Bureau of Comptroller and Global Financial Services (CGFS) shall be

consulted *concerning* the cost implications of proposed mitigation measures.

e. The Under Secretary of Management (M), pursuant to Delegation of Authority DA-198, or other duly delegated official, *makes* final decisions regarding notification of the breach. Notification, including provision of credit monitoring services, also may be made pursuant to bureau-specific procedures consistent with this policy and OMB M-07-16 requirements that have been approved in advance by the PPGB and/or the Under Secretary for Management (M).

# 5 FAM 468.6 Notification and Delayed Notification

## 5 FAM 468.6-1 Guidelines for Notification

*(CT:IM-156; 10-01-2014)*

a. *When bureaus or offices are tasked with* notifying individuals whose personal information is subject to a risk of misuse arising from a breach, *the Core Response Group (CRG) is responsible for ensuring that the bureau or office provides the following information:*

(1) *Describe briefly* what happened, including the date(s) of the breach and its discovery, if known;

(2) *Describe,* to the extent possible, the types of personal information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account numbers);

(3) *Explain briefly* action the Department is taking to investigate the breach, to mitigate harm, and to protect against any further breach of the data;

(4) *Provide contact* procedures for individuals wishing to ask questions or learn additional information to include a toll-free telephone number, an e-mail address, website, and/or postal address;

(5) *Explain steps* individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts (alerts of any key changes to such reports and on-demand personal access to credit reports and scores), if appropriate, and instructions for obtaining other credit protection services, such as credit freezes; and

(6) *Explain briefly* how the information was protected at the time of the breach.

b. In developing a mitigation strategy, the Department considers all available credit protection services and will extend such services in a consistent and fair manner. Affected individuals will be advised of the availability of such services, where appropriate, and under the circumstances, in the most expeditious manner possible, including but not limited to mass media distribution and broadcasts.

## 5 FAM 468.6-2 Means of Notification

*(CT:IM-156; 10-01-2014)*

a. Notification by first-class mail should be the primary means by which notification is provided. Exceptions to this *are* instances where there is insufficient or outdated contact information which would preclude direct written notification to an individual who is the subject of a data breach.

b. A substitute form of notice may be provided, such as a conspicuous posting on the Department's home page and notification in major print and broadcast media, including major media in geographic areas where the affected individuals likely reside. A notice in the media will include a toll-free telephone number *that* an individual can *call to inquire as to* whether his or her personal information is possibly included in the breach. Special consideration for accommodations should be consistent with Section 508 of the Rehabilitation Act of 1973 and may include the use of telecommunications devices for the hearing-impaired.

c. *If* it *is* determined that notification must be immediate, the Department may provide information to individuals by telephone, *e-mail*, or other means, as appropriate.

## 5 FAM 468.6-3 Delayed Notification Due to Security Considerations

*(CT:IM-156; 10-01-2014)*

a. Any request for a delay in notifying the affected subjects should state an estimated date after which the requesting entity believes notification will not adversely affect the conduct of the investigation, national security, or efforts to recover the data. Any delay should not *unduly* exacerbate risk or harm to any affected individuals. The Privacy Protection Governance Board (PPGB) *shall* be informed of a delayed notification.

b. Notwithstanding the foregoing, notifications may be delayed or barred upon a request from the Bureau of Diplomatic Security (DS) or other Federal entities or agencies in order to protect data, national security or computer resources from further compromise or to prevent interference with the conduct of a lawful investigation or efforts to recover the data.

## 5 FAM 468.7 Documenting Department Data Breach Actions

*(CT:IM-156; 10-01-2014)*

The Bureau of Administration (A), as appropriate, must document the Department’s responses to *data* breaches and must ensure that appropriate and

adequate records are maintained. These records must be maintained in accordance with *the Federal Records Act of 1950*.

# 5 FAM 469 RULES OF BEHAVIOR FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

## 5 FAM 469.1 Purpose

*(CT:IM-156; 10-01-2014)*

*a.* The Rules of Behavior contained herein are the behaviors all workforce members *must* adhere to in order to protect the personally identifiable information (PII) they have access to in the performance of their official duties. The Federal Information Security Management Act (FISMA) of 2002 requires system owners to ensure that individuals requiring access to information and information technology (IT) systems, including those containing PII, sign appropriate access agreements prior to being granted access. The access agreement for a system must include rules of behavior tailored to the requirements of the system.

*b. All Department workforce members are required to complete the Cyber Security Awareness course (PS800) annually. This course contains a privacy awareness section to assist employees in properly safeguarding PII. Additionally, there is the Foreign Service Institute distance learning course, Protecting Personally Identifiable Information (PII) (PA459). This is a one-time mandatory requirement for all Foreign Service employees, Civil Service employees, and locally employed staff who handles PII while performing their official Department duties.*

## 5 FAM 469.2 Responsibilities

*(CT:IM-156; 10-01-2014)*

a. Executive directors or equivalent are responsible for protecting personally identifiable information (PII) by:

(1) Ensuring workforce members who handle records containing PII adhere to legal, regulatory, and *Department* policy requirements regarding privacy;

(2) Determining the risks and effects of collecting, maintaining, and disseminating PII in a system;

(3) Taking appropriate action when they discover or suspect failure to follow the rules of behavior for handing PII;

(4) *Conducting an administrative fact-finding task to obtain all pertinent*

*information relating to a suspected or confirmed breach of PII;*

(*5*) Allocating adequate budgetary resources to protect PII, including technical measures or procedures requiring encryption, secure remote access, etc.; and

(*6*) Executing other responsibilities related to PII protections specified on the Chief Information Security Officer (CISO) and Privacy websites.

b. Supervisors are responsible for protecting PII by:

(1) Implementing rules of behavior for handling PII;

(2) Ensuring their workforce members receive the training necessary to safeguard PII;

(3) Taking appropriate action when they discover or suspect failure to follow the rules of behavior for handling PII; and

(4) Executing other responsibilities related to PII protections specified at the Chief Information Security Officer (CISO) and Privacy websites.

c. Workforce members are responsible for protecting PII by:

(1) Not accessing records for which they do not have a "need to know" or those records which are not specifically relevant to the performance of their official duties (see 5 FAM 471, subparagraph a(2));

(2) Not disclosing sensitive PII to individuals or outside entities unless they are authorized to do so as part of their official duties and doing so is in accordance with the provisions of the Privacy Act of 1974, as amended, and Department privacy policies;

(3) Not correcting, altering, or *updating* any sensitive *PII* in official records except when necessary as part of their official duties; and

(4) Executing other responsibilities related to PII protections specified at the Chief Information Security Officer (CISO) and Privacy websites.

## 5 FAM 469.3 Limitations on Removing Personally Identifiable Information (PII) From Networks and Federal Facilities

*(CT:IM-156; 10-01-2014)*

a. Removing personally identifiable information (PII) from Federal facilities risks exposing it to unauthorized disclosure. Do not remove or transport sensitive *PII* from a Federal facility unless it is essential to the performance of your official duties. If it is essential, obtain supervisory approval before removing records containing sensitive *PII* from a Federal facility. Any PII removed should be the minimum amount necessary to accomplish your work and, when required to return records to that facility, you must return the sensitive

personally identifiable information promptly.

b. Transmitting PII electronically outside the Department's network via the Internet may expose the information to unauthorized access. Workforce members who have a valid business need to do so are expected to comply with 12 FAM 544.3. Otherwise, sensitive *PII* in electronic form must be encrypted using the encryption tools provided by the Department, when transported, processed, or stored off-site. (See 5 FAM 469.3 paragraph c and Chief Information Security Officer's toolkit Website.)

c. Storing and processing sensitive *PII* on any non-U.S. Government computing device and/or storage media (e.g., personally-owned or contractor-owned computers) is strongly discouraged and should only be done with the approval from the appropriate bureau's executive director, or equivalent level. Encryption standards for personally-owned computers and removable storage media (e.g., a hard drive, compact disk, etc.) can be found in 12 FAM 682.2-4.

## 5 FAM 469.4 Avoiding Technical Threats to Personally Identifiable Information (PII)

*(CT:IM-156; 10-01-2014)*

a. **Computer based threats:**

(1) Protect your computer in accordance with the computer security requirements found in 12 FAM 600;

(2) Protect access to all PII on your computer from anyone who does not have a "need-to-know" in order to execute their official duties;

(3) Logoff or lock your computer before leaving it unattended; and

(4) Shield your computer from unauthorized viewers by repositioning the display or attaching a privacy screen.

b. **Password protection:**

(1) Protect your computer passwords and other credentials (e.g., network passwords for specific network applications, encryption, etc.) in accordance with the requirements stated in 12 FAM 622.1-3 and 12 FAM 632.1-4;

**NOTE**: This applies not only to your network password but also to passwords for specific applications, encryption, etc

(2) Use a complex password for unclassified and classified systems as detailed in 12 FAM 623.3-1 and 12 FAM 632.1-4, respectively;

(3) Do not reveal your password to others (see 12 FAM 622.1-3 paragraph n); and

(4) Do not use your password when/where someone might see and remember it (see 12 FAM 622.1-3 paragraph n).

c. **Threats to data at rest:**

(1) Do not post or store sensitive personally identifiable information *(PII)* in shared electronic or network folders/files that workforce members without a "need to know" can access;

(2) Storing sensitive *PII* on U.S. Government-furnished mobile devices and removable media is permitted if the media is encrypted. Unclassified media must be encrypted to the Federal Information Processing Standards (FIPS) 140-2, or later National Institute of Standards and Technology (NIST) standard. The Information Technology *Configuration* Control Board (IT CCB) must also approve the encryption product;

(3) At Department facilities (e.g., official duty station *or* office), store hard copies containing sensitive *PII* in locked containers or rooms approved for storing Sensitive But Unclassified (SBU) information (for further guidance, see 12 FAM 544.1); and

(4) Do not leave sensitive *PII* unsecured or unattended in public spaces (e.g., unsecured at home, left in a car, checked-in baggage, left unattended in a hotel room, etc.).

d. **Remote access:** Use the *Department's approved method for the secure remote access of PII on the Department's SBU network,* from any Internet-connected computer meeting the system requirements*. For further guidance regarding remote access, see* 12 FAM 680*.*

e. **Voice and mail transmissions:**

(1) Protect against eavesdropping during telephones calls or other conversations that involve PII;

(2) Mailing sensitive PII to posts abroad should be done via the Diplomatic Pouch and Mail Service where these services are available (refer to 14 FAM 720 and 14 FAM 730, respectively, for further guidance); and

(3) When mailing records containing sensitive *PII* via the U.S. Postal Service (USPS) or a commercial carrier or foreign postal system, senders should use trackable mailing services (e.g., Priority Mail with Delivery Confirmation, Express Mail, or the commercial/foreign equivalent). In some cases, the sender may also request a signature from the recipient (refer to 14 FAM 730, Official Mail and Correspondence, for additional guidance).

## 5 FAM 469.5 Destroying and Archiving Personally Identifiable Information (PII)

*(CT:IM-156; 10-01-2014)*

a. Destroy and/or retire records in accordance with your office's Records Disposition Schedule. Work with your organization's records coordinator to

implement the procedures necessary in performing these functions. The Disposition Schedule covering your organization's records can be accessed at the Records Management website. *PII is Sensitive But Unclassified (SBU) information as defined in* 12 FAM 540. *PII to be destroyed, that is part of an official record, unofficial record, or copy, created by a workforce member, must be destroyed by shredding, burning, or by other methods consistent with law or regulation as stated in* 12 FAM 544.1, *Fax Transmission, Mailing, Safeguarding/Storage, and Destruction of SBU*.

b. Further guidance is provided in 5 FAM 430, Disposition of Records, *and* 12 FAM 540, *Sensitive But Unclassified Information.*

## 5 FAM 469.6 Consequences for Failure to Safeguard Personally Identifiable Information (PII)

*(CT:IM-156; 10-01-2014)*

a. Violations or possible violations must be processed as prescribed in the Privacy Act of 1974, as amended. Violations may constitute cause for appropriate penalties including but not limited to:

(1) Criminal prosecution, *as set forth in section (i) of the Privacy Act*;

(2) Administrative action (e.g., removal or other adverse personnel action). Workforce members will be held accountable for their individual actions. In certain circumstances, consequences for failure to safeguard personally identifiable information (PII) or respond appropriately to a *data* breach could include disciplinary action. Additionally, such failure could be addressed in individual performance evaluations, contract performance evaluations, or may result in contractor removal. Supervisors who are aware of *a subordinate's data breach involving* PII and allow such conduct to continue may also be held responsible for failure to provide effective organizational security oversight; and

(3) Nondisciplinary action (e.g., removal of authority to access information or information systems) for workforce members who demonstrate egregious disregard or a pattern of error for safeguarding PII.

b. An executive director or equivalent is responsible for:

(1) Identifying behavior that does not protect PII as set forth in this subchapter;

(2) Documenting and addressing the behavior, as appropriate;

(3) Notifying the appropriate authorities if the workforce members belong to other organizations, agencies or commercial businesses; and

(4) Reporting the results of the inquiry to the Senior Agency Official for Privacy (SAOP) and the Chief Information Security Officer (CISO).